数据权限管理方案

技术工程部-数据组-曹娜

邮箱：caona02@meituan.com

目录

- 数据权限管理现状
- 数据权限管理方案
- 报表/指标/维度值的权限管理方案介绍
- 未来的规划

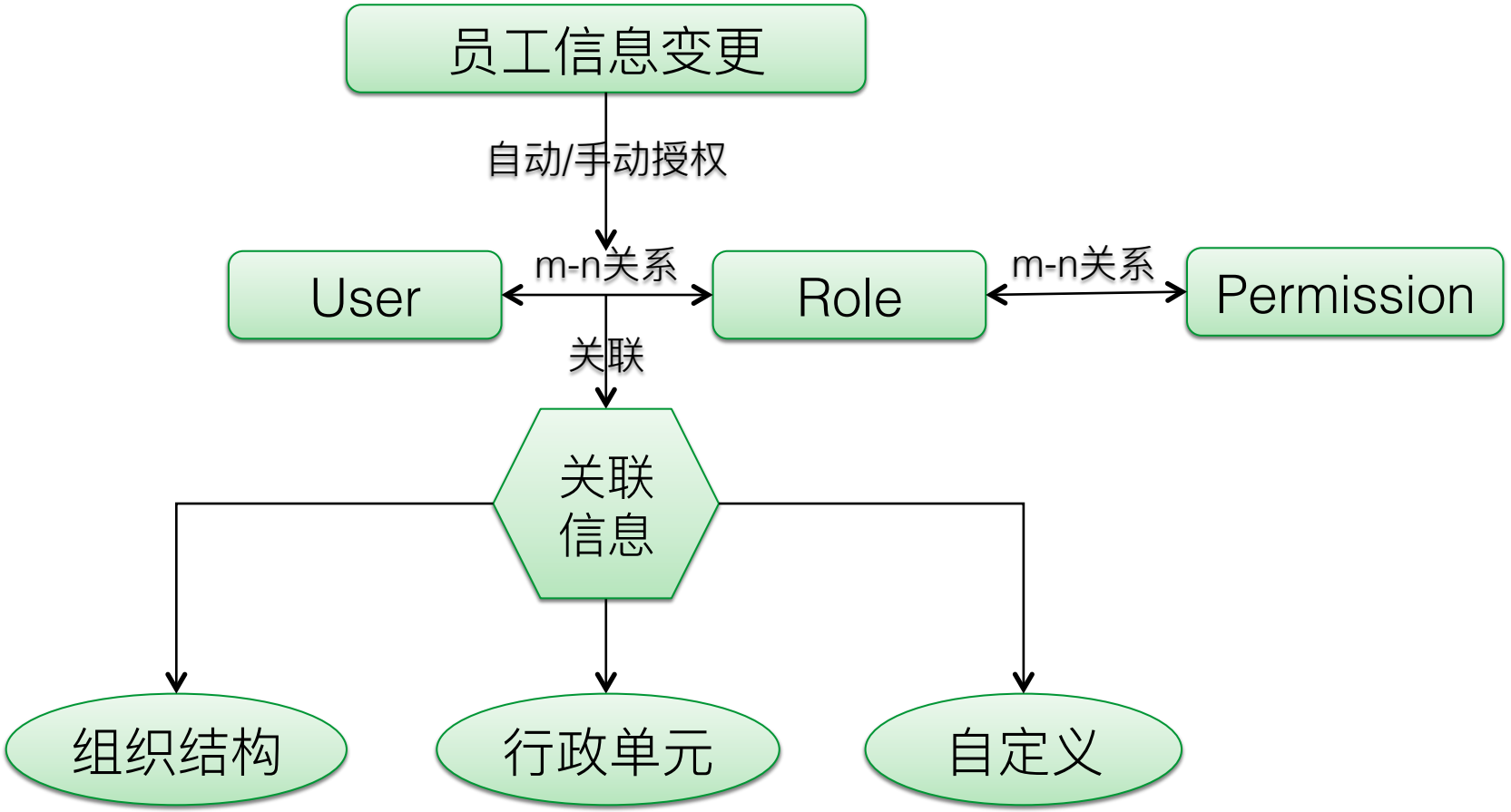
目录

数据权限管理现状

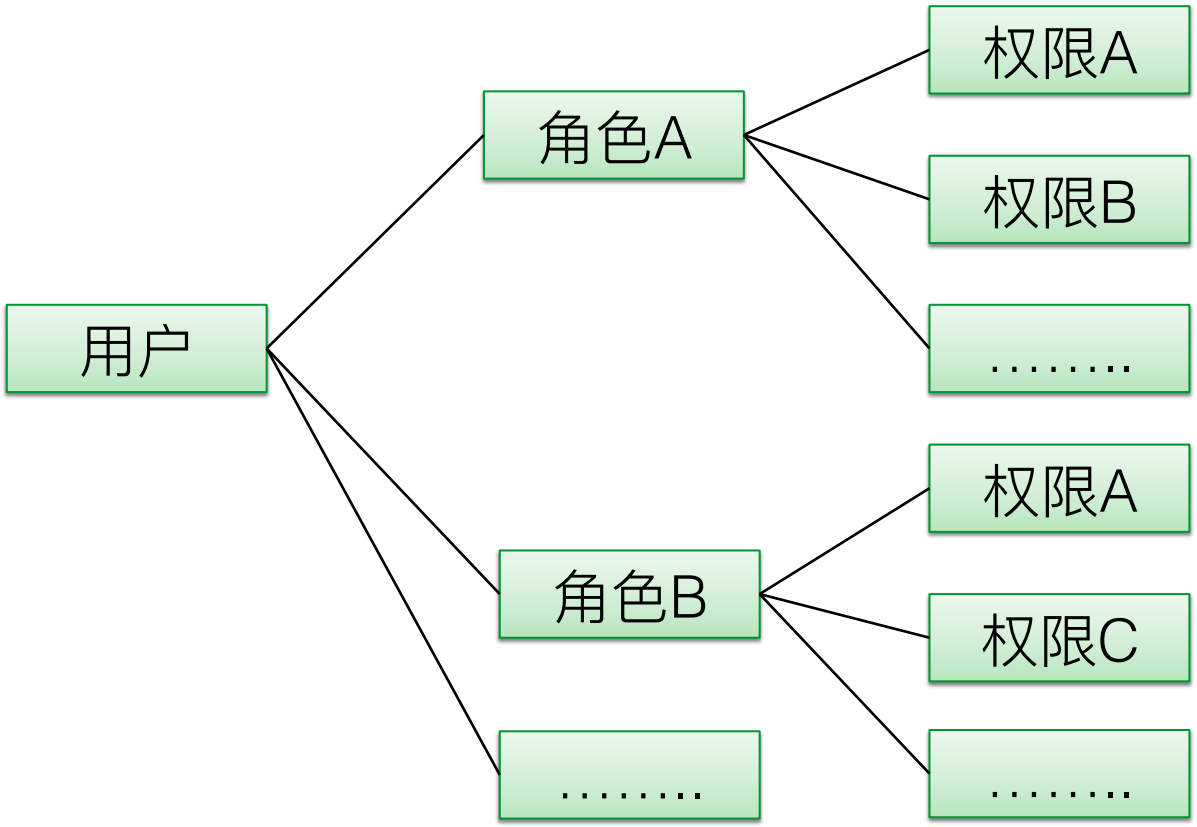
如下权限如何申请?

用户A由于工作需要 申请报表A、报表B的权限，报表申请只读权限，该走什么样的流程呢?

权限基本模型(RBAC)

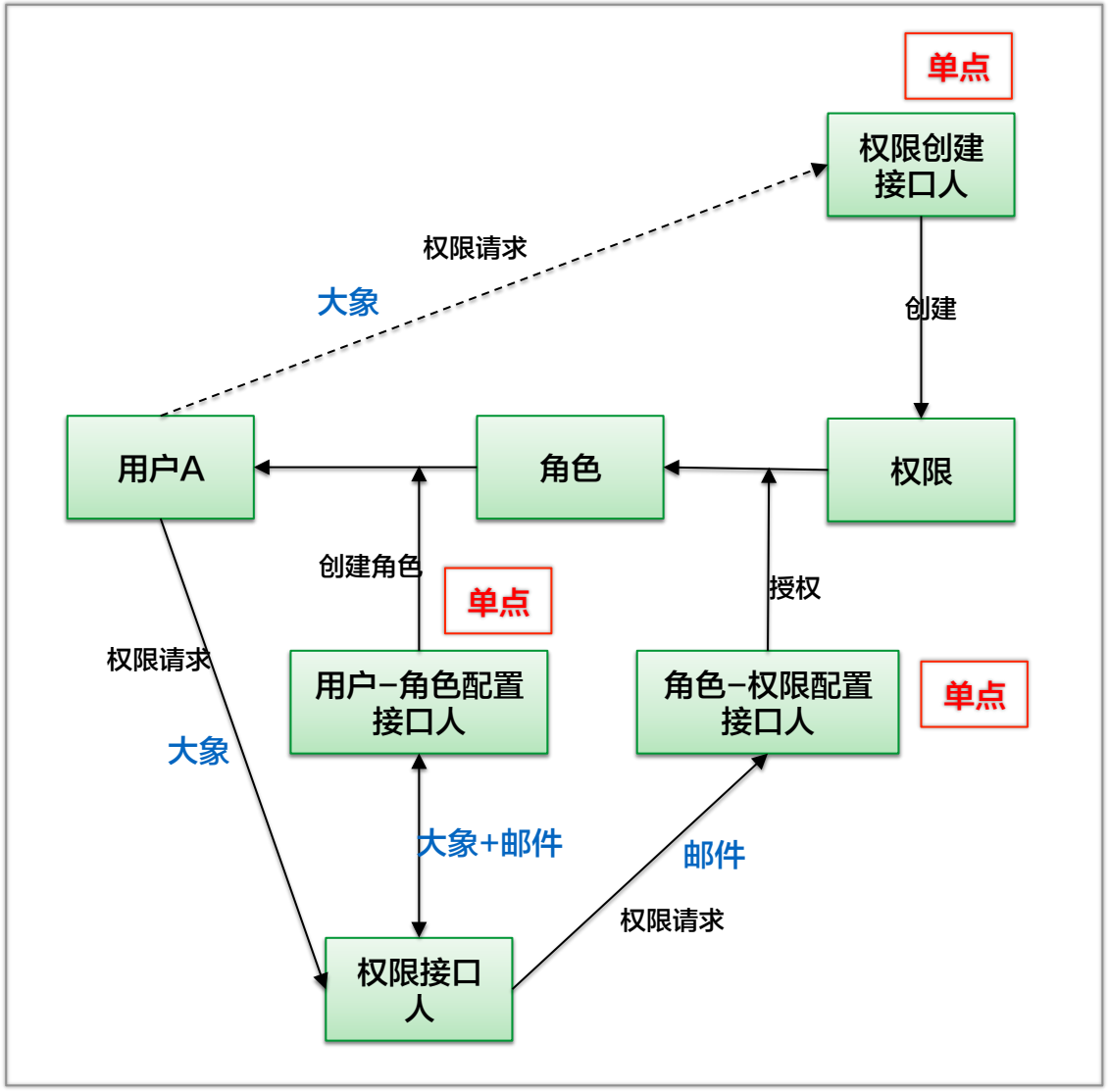

员工信息变更
自动/手动授权
User
m-n关系
Role
m-n关系
Permission
关联
关联
信息
组织结构
行政单元
自定义

权限分配机制



备注：系统不支持直接给用户配置权限，用户只能通过配置角色来获得权限

申请/授权流程



用户权限过大

流程长，且有单点问题

组织架构、岗位调整导致权限丢失

不可审计

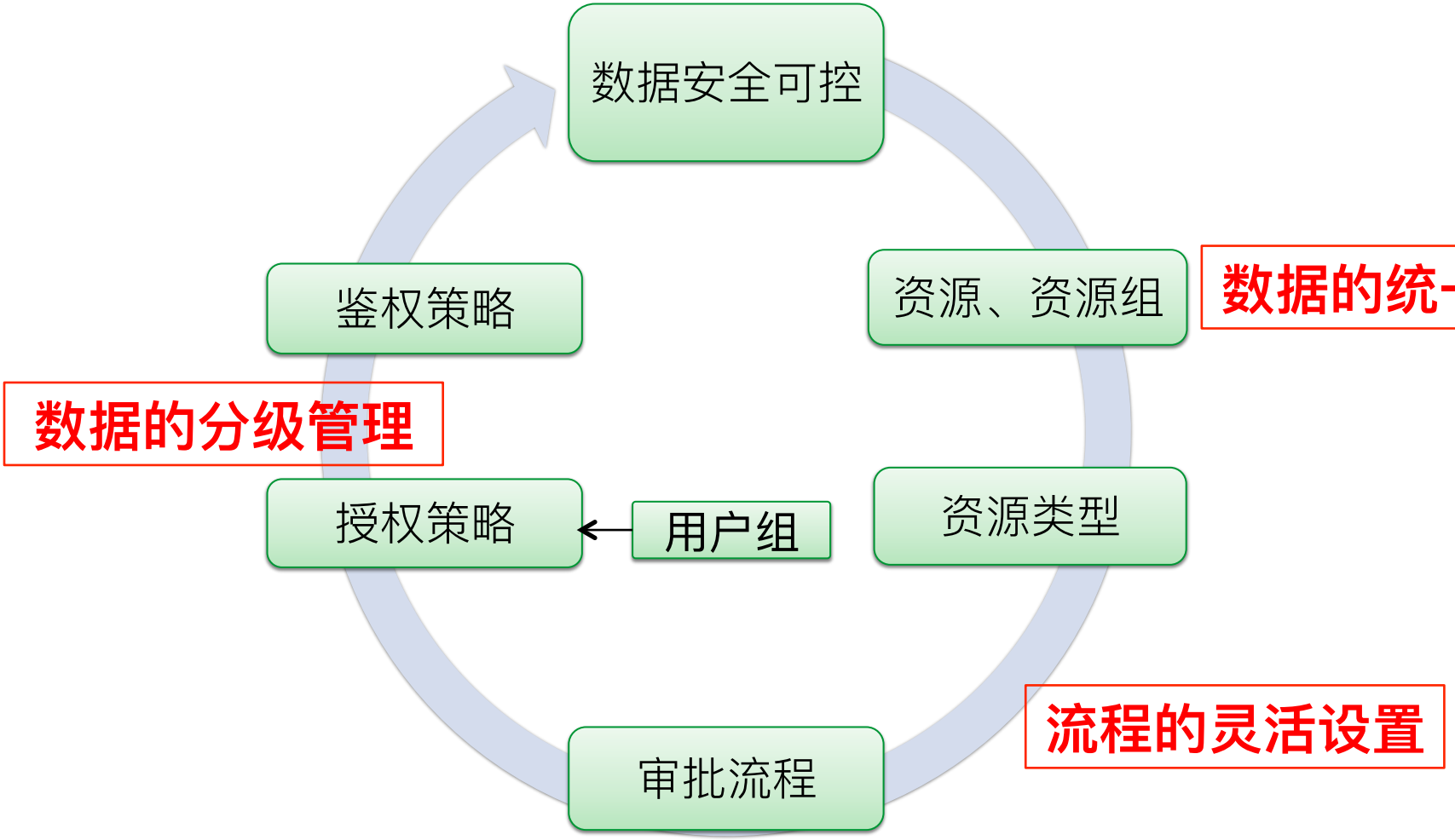
目录

- 数据权限管理现状
- 数据权限管理方案
- 报表/指标/维度值的权限管理方案介绍
- 未来的规划

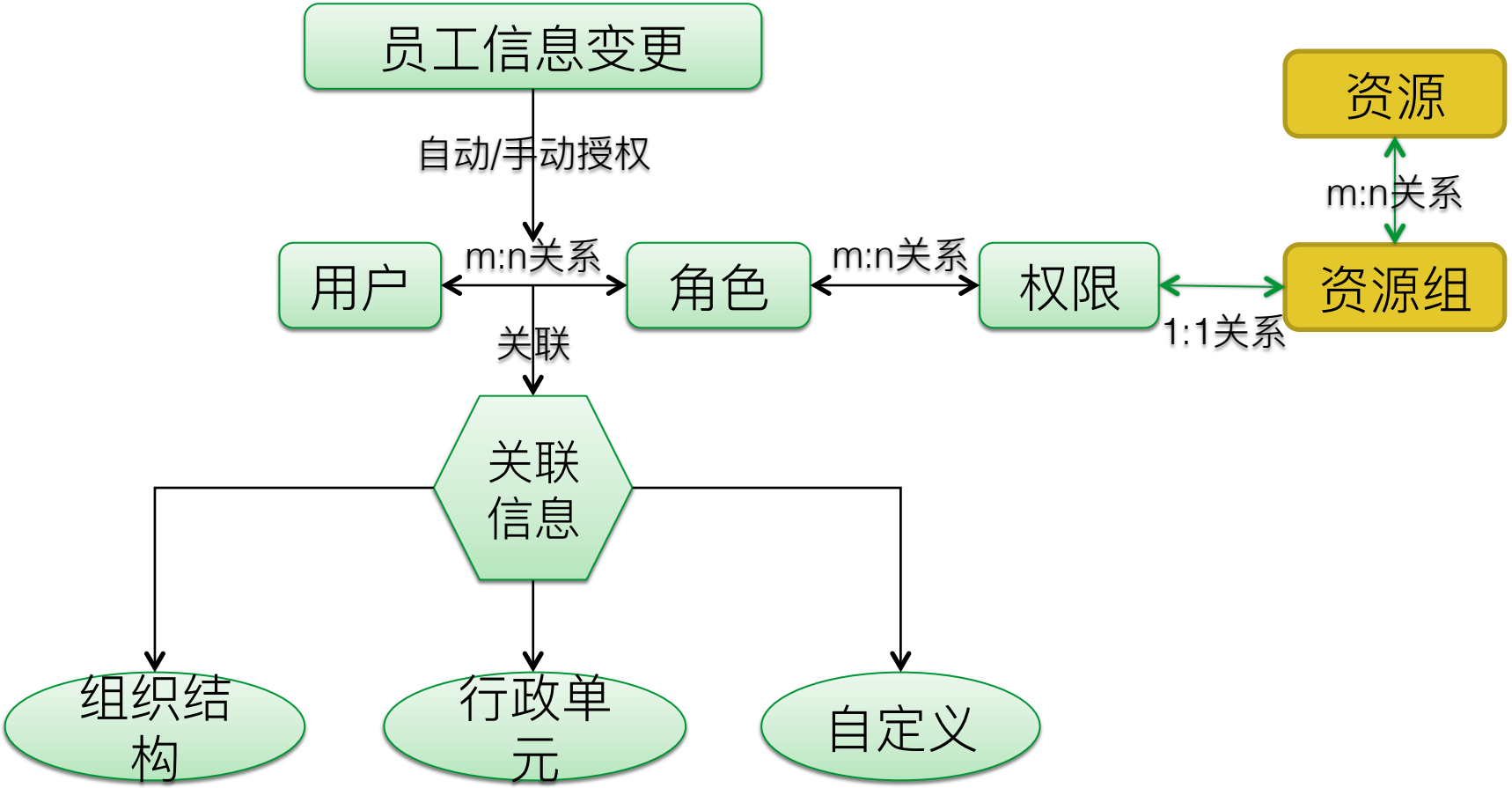
目标

- 制定公司统一的数据安全等级划分的指导准则
- 建设简单、灵活的数据权限管理系统，达到数据安全可控、缩短用户申请时长，支持审计功能

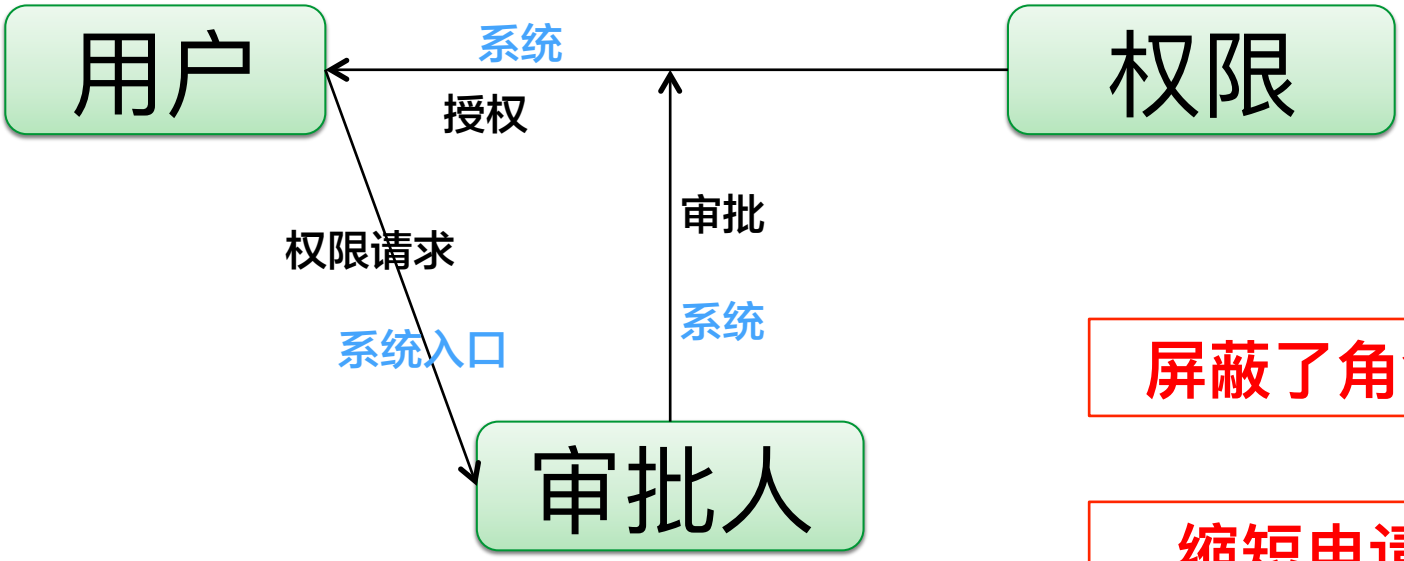
数据权限管理思路


数据安全可控
资源、资源组
数据的统一表示
资源类型
流程的灵活设置
审批流程
用户组
授权策略
数据的分级管理
鉴权策略

改进后的权限基本模型


员工信息变更
自动/手动授权
用户
m:n关系
角色
m:n关系
权限
1:1关系
资源
m:n关系
资源组
关联
关联信息
组织结构
行政单元
自定义

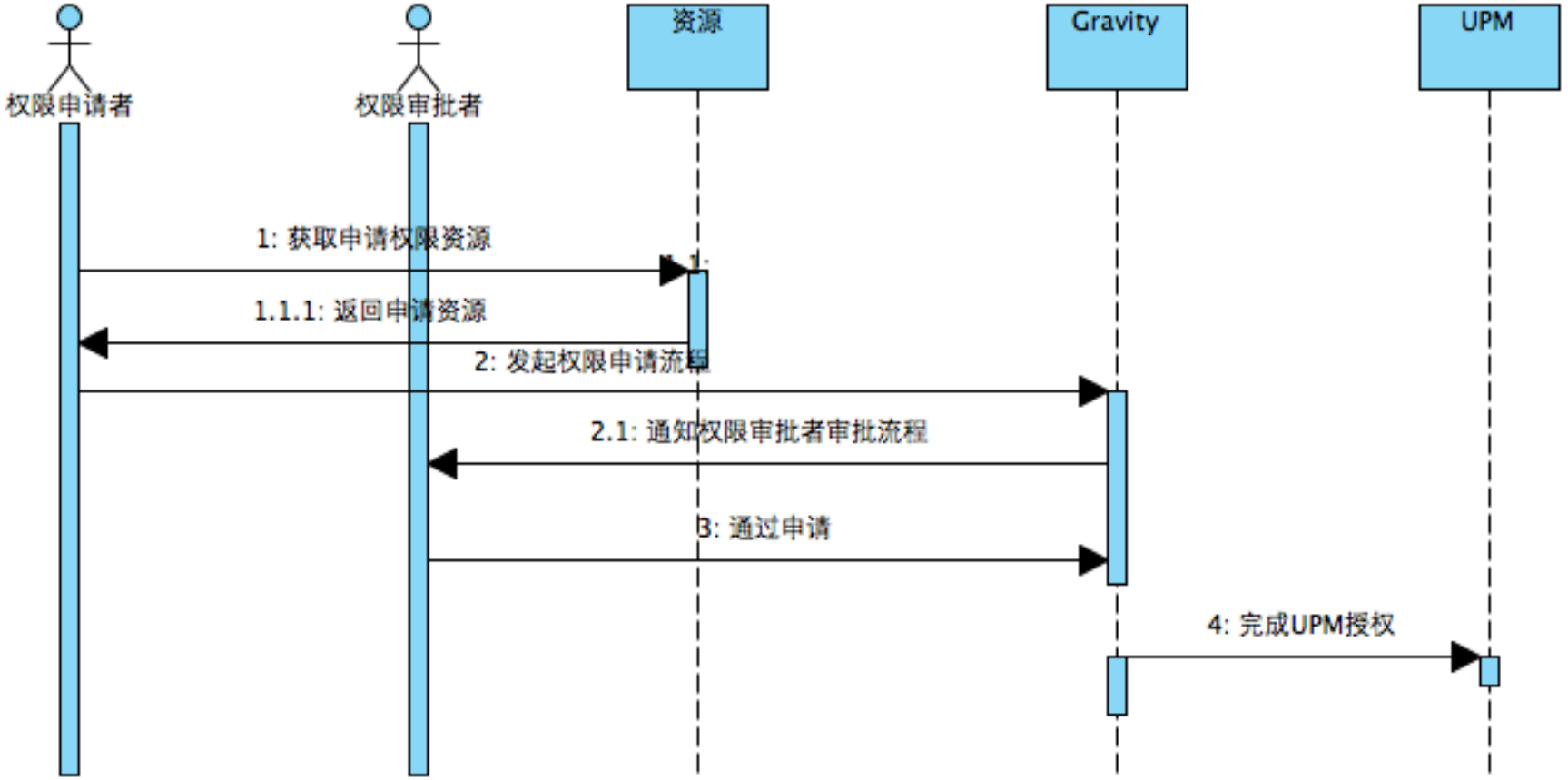
申请/授权流程



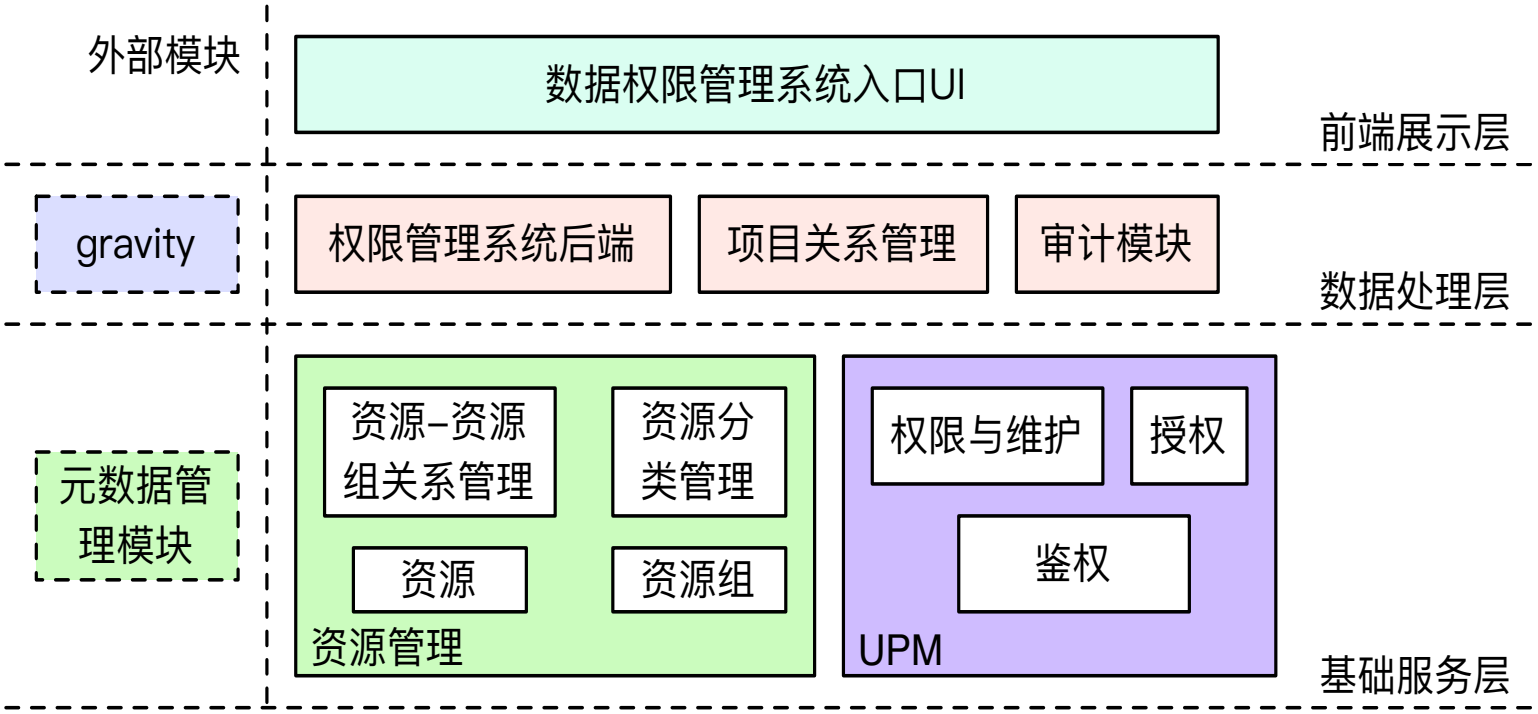
屏蔽了角色概念

缩短申请时长

权限申请用例图


权限申请者
权限审批者
资源
Gravity
UPM
1: 获取申请权限资源
1.1.1: 返回申请资源
2: 发起权限申请流程
2.1: 通知权限审批者审批流程
3: 通过申请
4: 完成UPM授权

系统模块划分

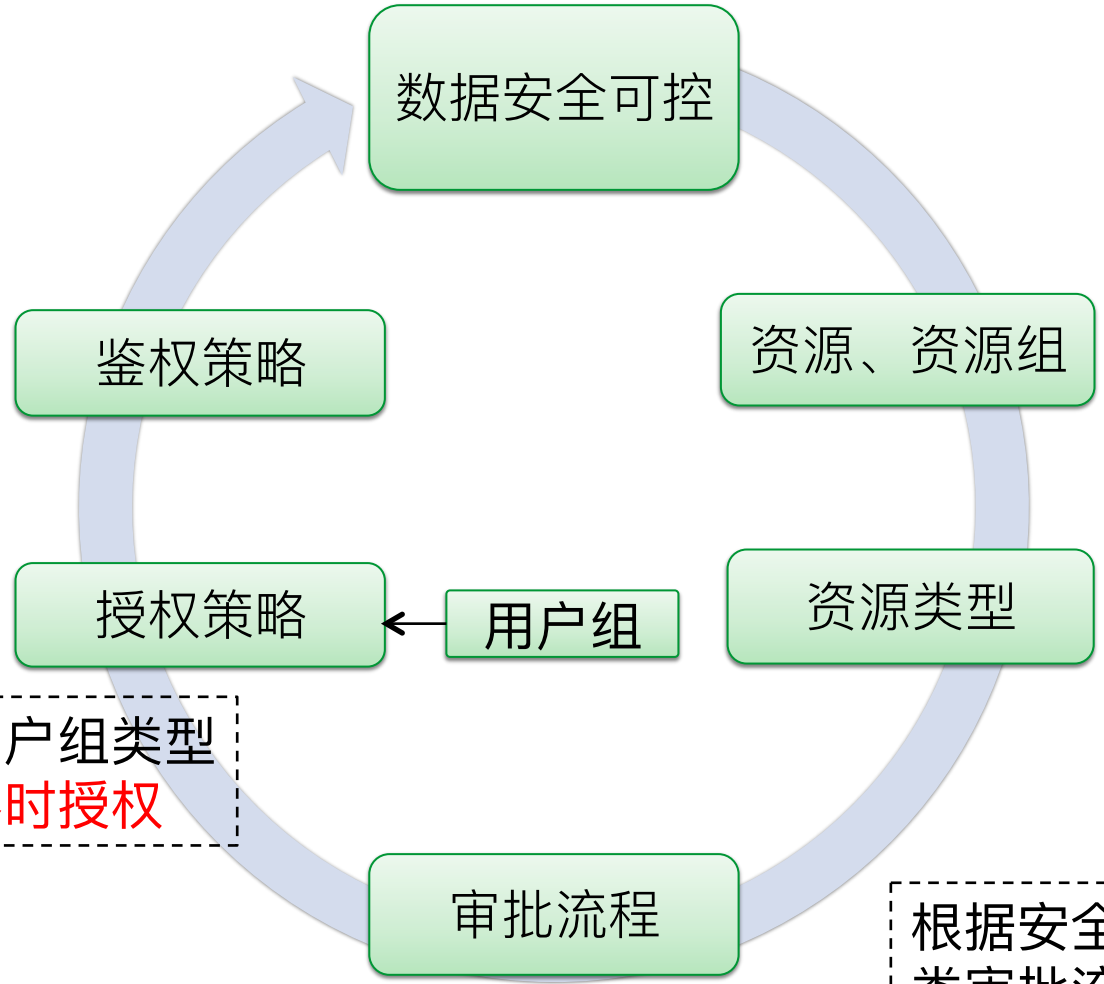

外部模块
数据权限管理系统入口UI
前端展示层
gravity
权限管理系统后端
项目关系管理
审计模块
数据处理层
元数据管理模块
资源-资源组关系管理
资源分类管理
资源
资源组
资源管理
权限与维护
授权
鉴权
UPM
基础服务层

目录

- 数据权限管理现状
- 数据权限管理方案
- 报表/指标/维度值的权限管理方案介绍
- 未来的规划

报表权限管理方案

报表权限管理思路



报表、资源、资源组
一一对应

按照安全等级划分类型，确定数据分级机制

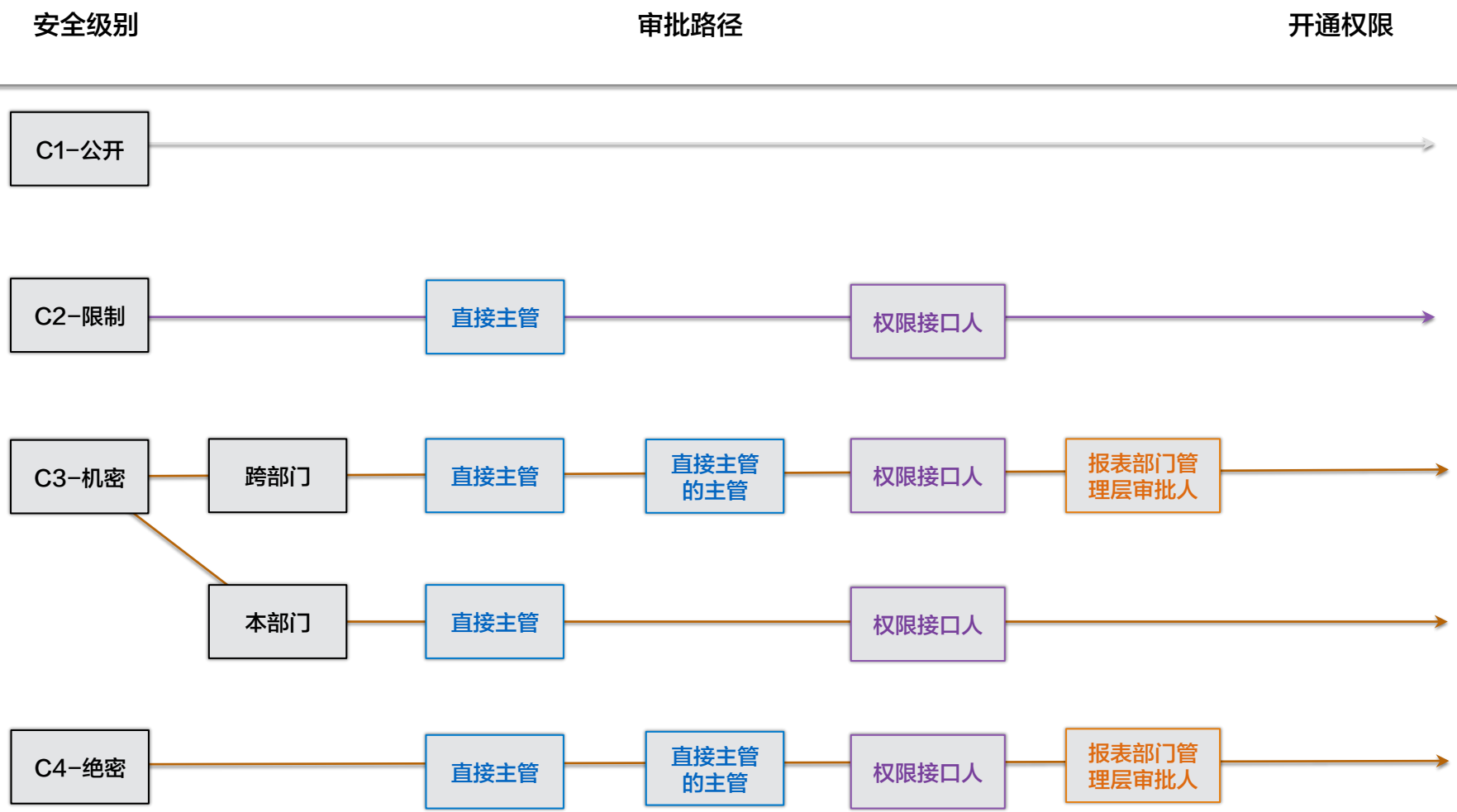
根据安全等级定制了3类审批流程，5种组合

根据用户组类型
实现零时授权

数据分级机制

安全等级	分级依据
C1(不限制)	适合于公开的数据，并不影响对外发布的数据
C2(限制)	不适合对外公开，但是对公司内部人员访问基本无限制
C3(机密)	适合于部分人可见的数据，丢失或不当使用将显著影响部门开展业务和提供服务等
C4(绝密)	仅适用于极少部分人可见，信息不安全可能导致公司面临法律或合规的风险

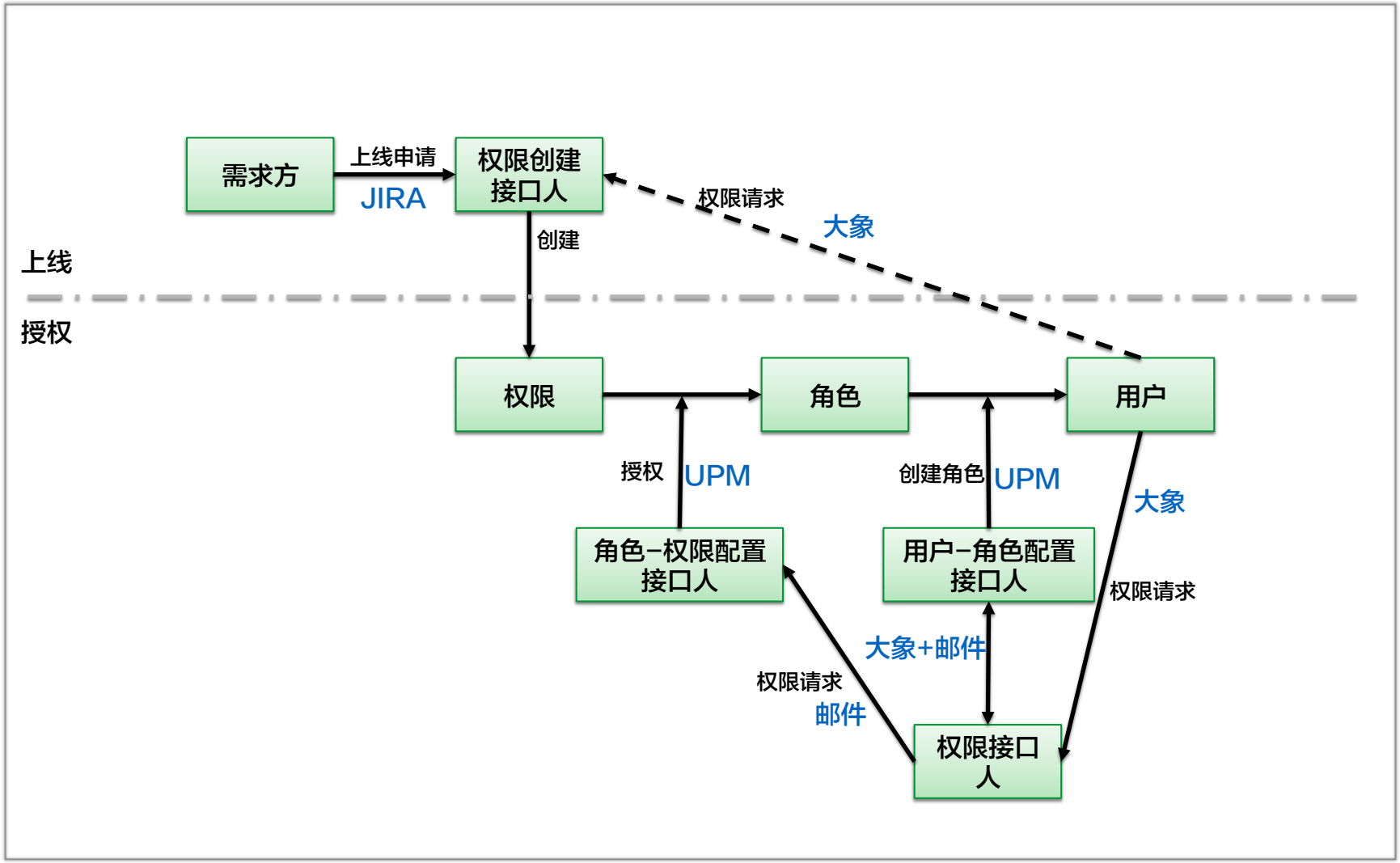
安全等级与审批流程关系



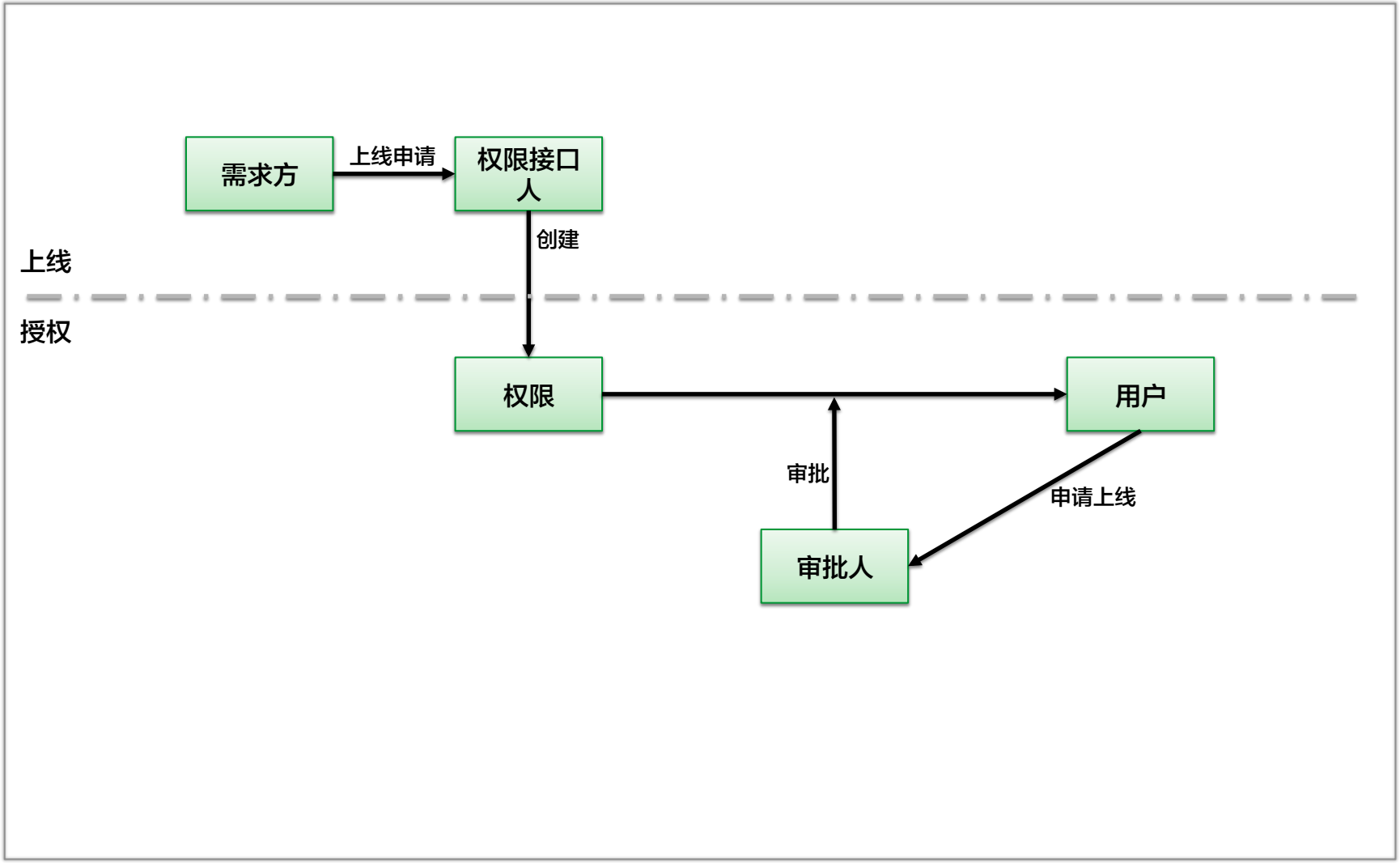
授权策略

用户组类别	授权策略
个人	C1级别由系统实现自动授权 C2及以上安全等级权限需要用户自行申请，并执行严格的审批流程
组织	根据用户与组织节点关系，由系统实现自动授权与撤销权限
岗位	根据用户与组织架构和岗位的关系，由系统实现自动授权与权限调整
项目	根据用户与项目关系，由系统实现自动授权与撤销权限

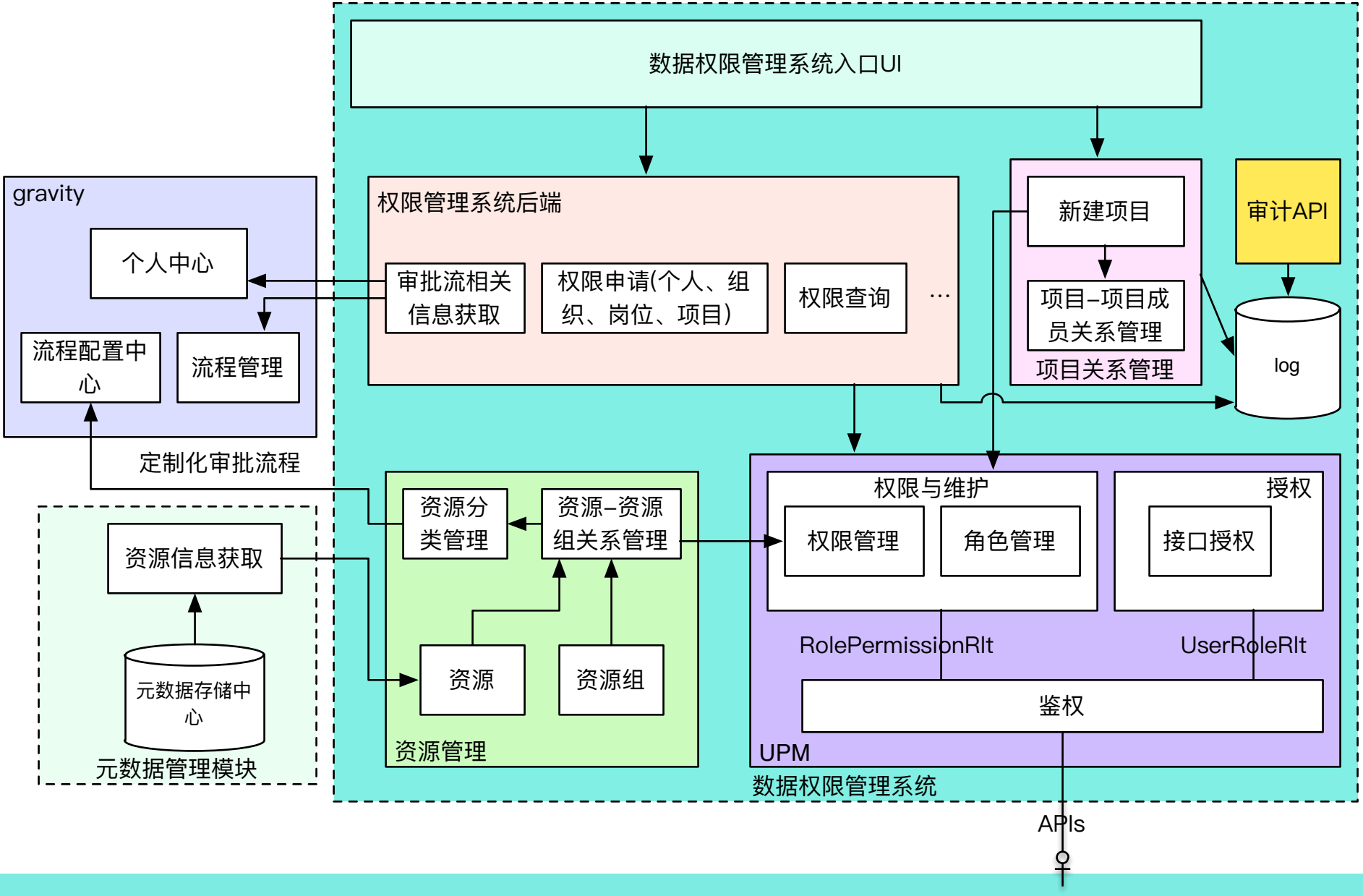
报表从上线到授权流程-上线前



报表从上线到授权流程-上线后



技术实现方案


数据权限管理系统入口UI
gravity
个人中心
流程配置中心
流程管理
定制化审批流程
权限管理系统后端
审批流相关信息获取
权限申请(个人、组织、岗位、项目)
权限查询
…
新建项目
项目–项目成员关系管理
项目关系管理
审计API
log
资源分类管理
资源–资源组关系管理
资源
资源组
资源管理
资源信息获取
元数据存储中心
元数据管理模块
权限与维护
权限管理
角色管理
授权
接口授权
RolePermissionRlt
UserRoleRlt
鉴权
UPM
数据权限管理系统
APIs

报表权限管理系统

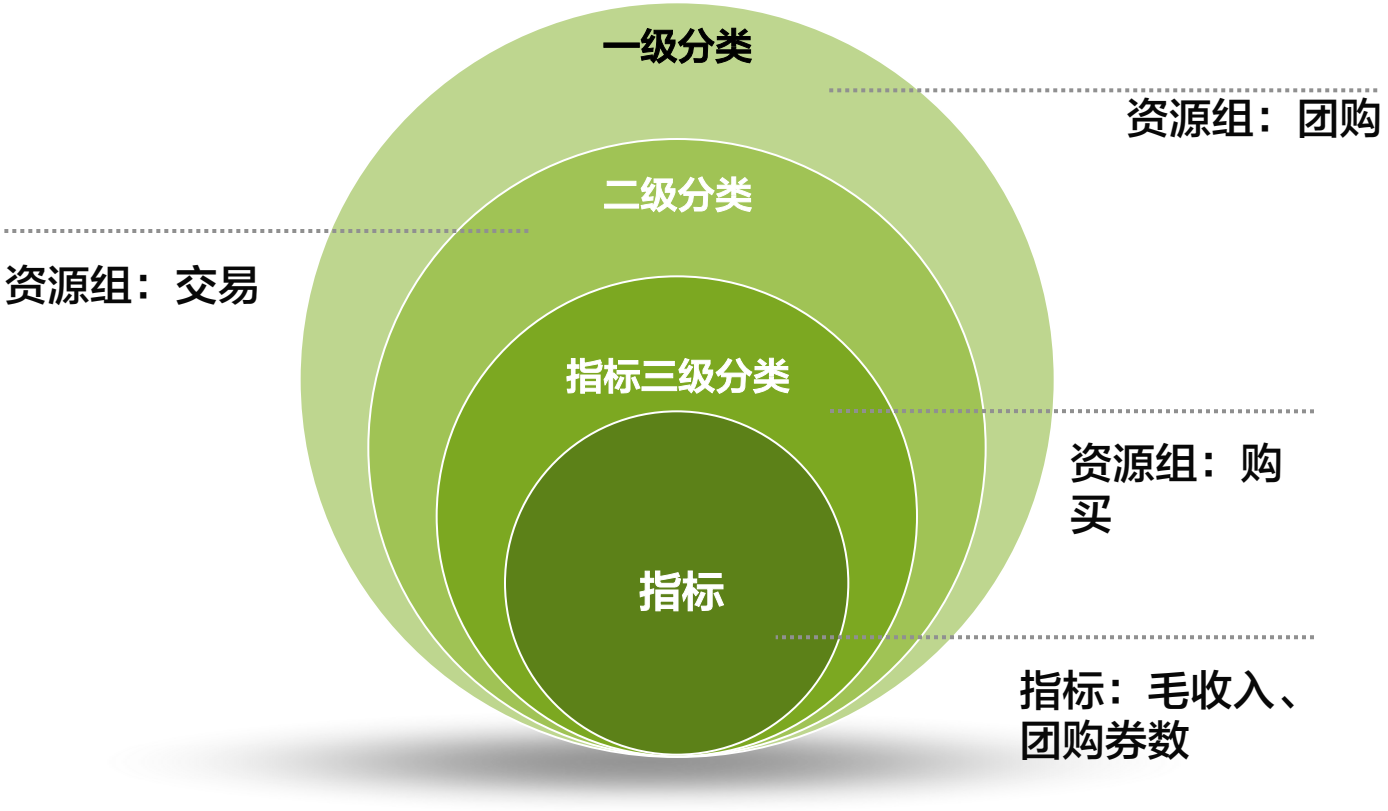

报表权限列表
个人权限申请
组织权限申请
项目权限申请
权限审批管理
报表上线申请
报表上线审批
项目关系管理
权限查询
管理员设置
FAQ
报表权限列表
筛选权限
权限状态
已授权
申请中
无权限
安全等级
C1 公开
C2 限制
C3 部门限制
C4 保密
搜索权限
请输入要搜索的权限
搜索
权限列表
ETL

报表权限管理系统

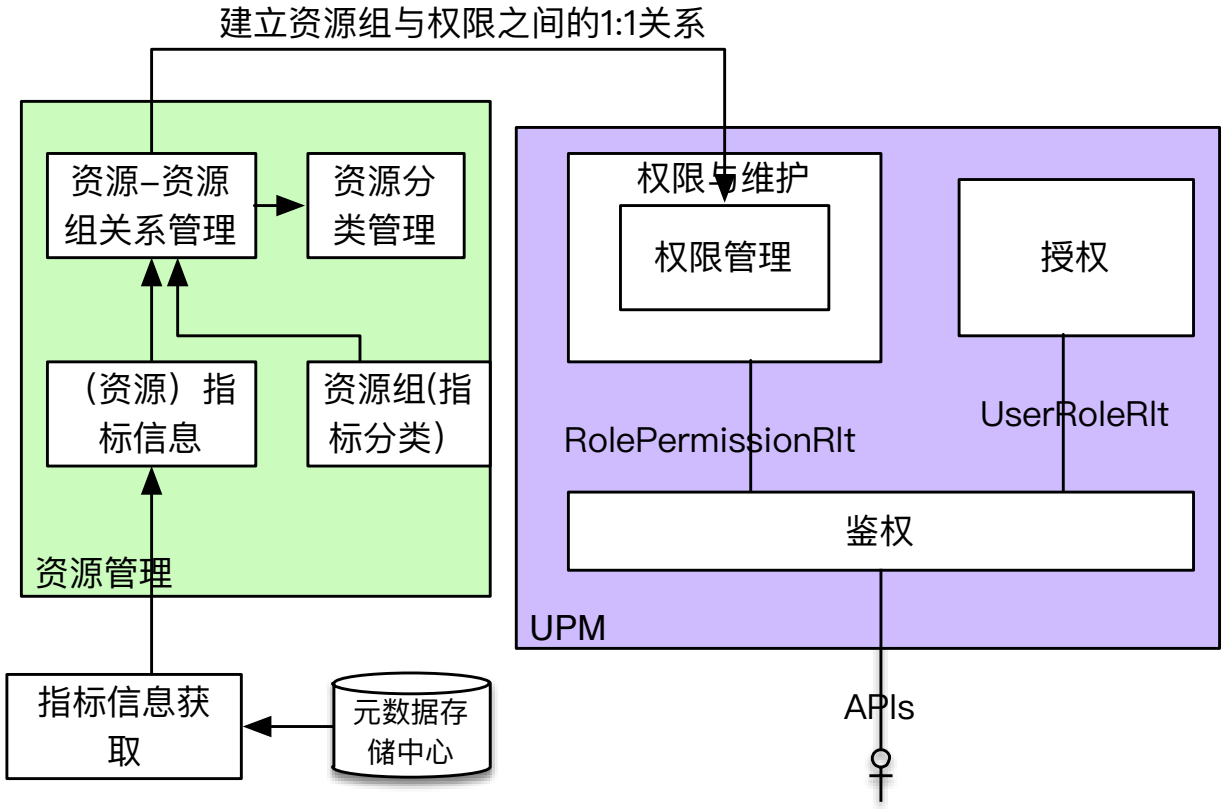

报表权限列表
个人权限申请
组织权限申请
项目权限申请
权限审批管理
报表上线申请
报表上线审批
项目关系管理
权限查询
管理员设置
FAQ
权限查询
按权限查用户
按用户查权限
选择要查询的权限
请输入要搜索的权限
搜索
个人
组织
组织岗位
项目
项目个人
请先选择用户类型 :-)
安全等级
C1
C2
C3
C4
ETL
报表名称
安全等级
管理

字段/指标级别的权限管理方案

资源-资源组关系-以指标为例



关键技术实现方案-以指标为例

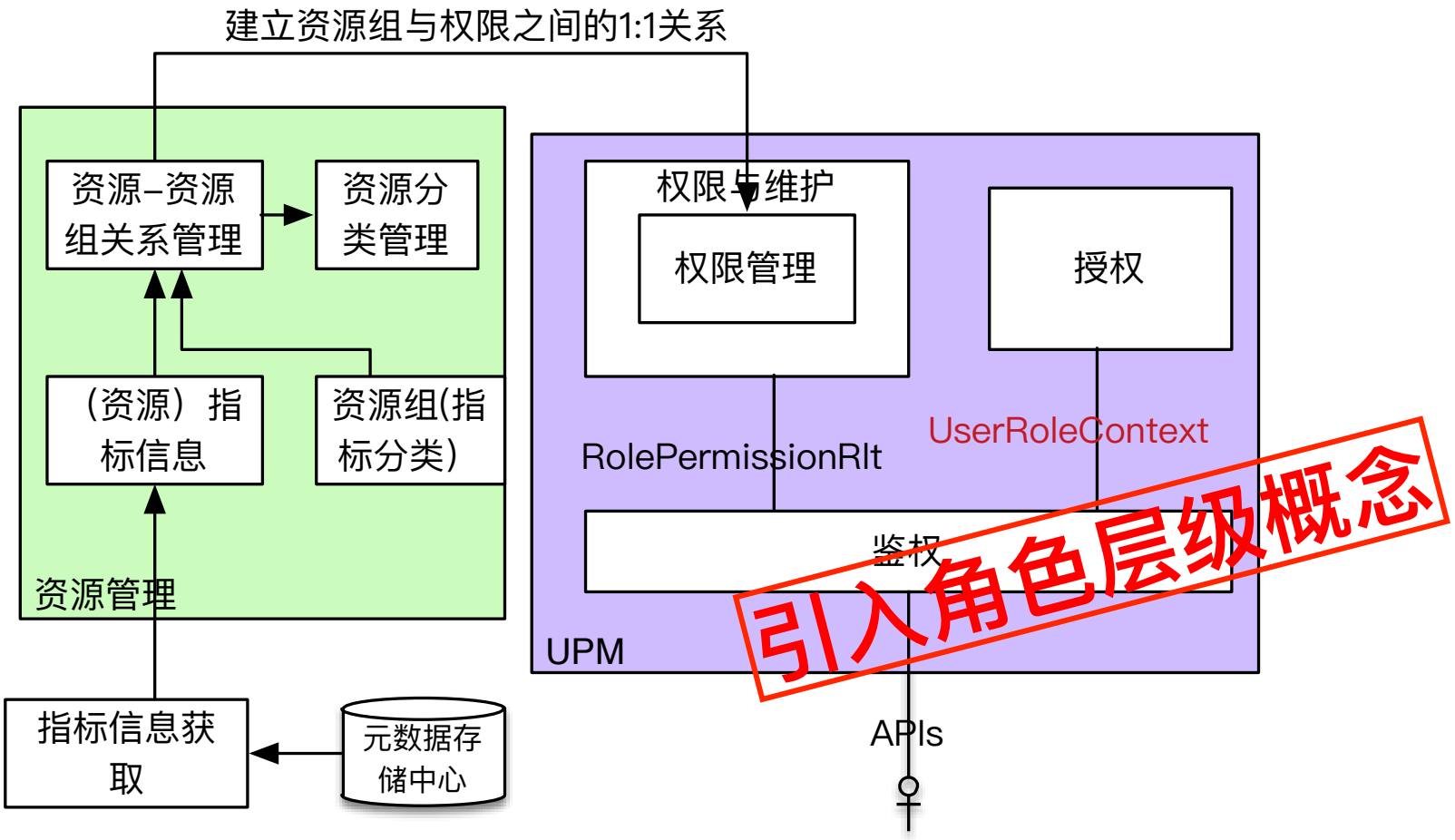


备注：

- 进行更新操作，根据资源与资源对应关系发生的变化，同时删除过时资源和资源组的关系
- 添加资源到对应的资源组中时，只添加之前不存在的资源，否则添加资源会有出错提示

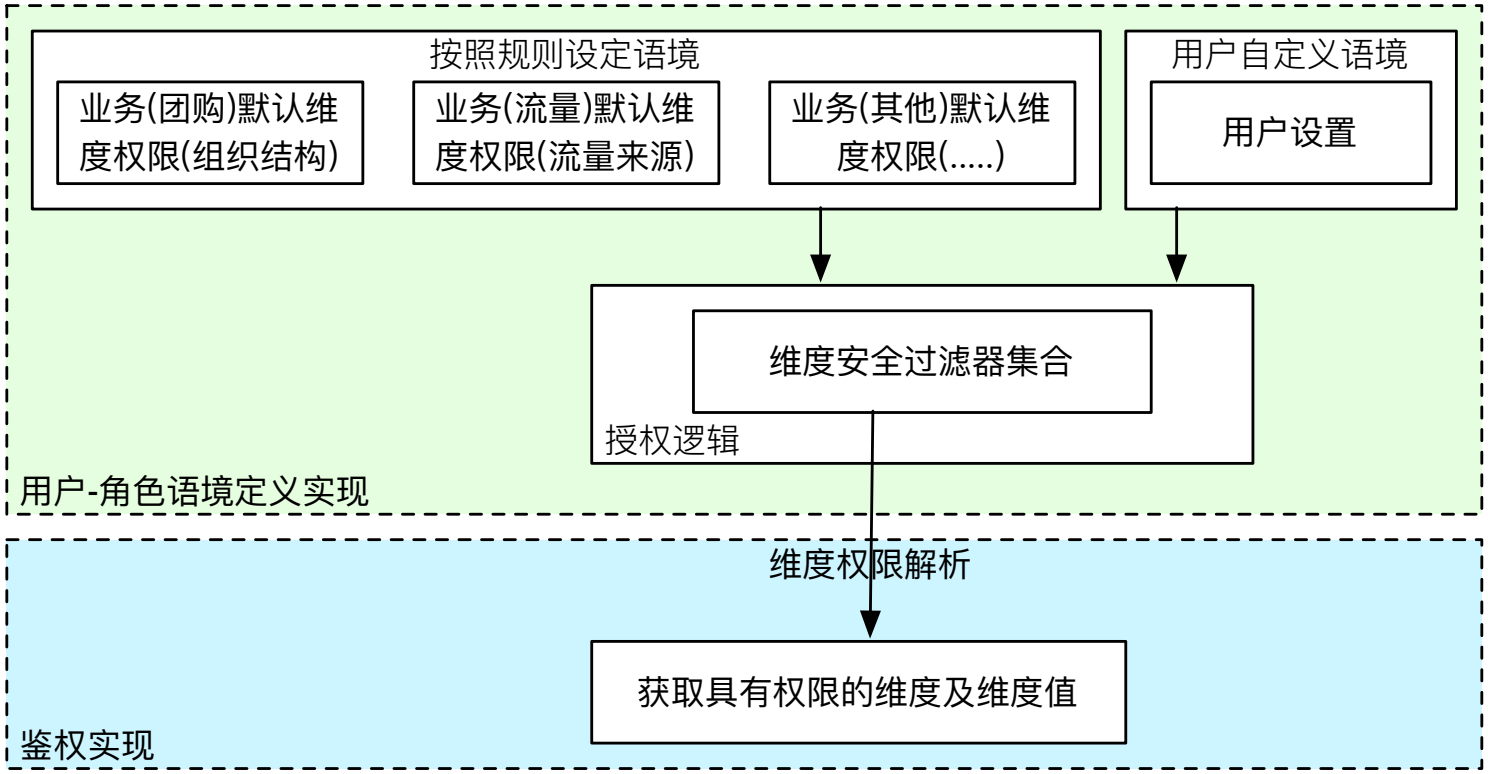
字段/维度阈值级别的权限管理方案

关键技术实现方案


建立资源组与权限之间的1:1关系
资源-资源组关系管理
资源分类管理
（资源）指标信息
资源组(指标分类)
资源管理
指标信息获取
元数据存储中心
权限与维护
权限管理
授权
RolePermissionRlt
UserRoleContext
鉴权
UPM
APIs
引入角色层级概念

UserRoleContext介绍

- 支持范围：按照规则设定语境、用户自定义语境
- 实现方式：

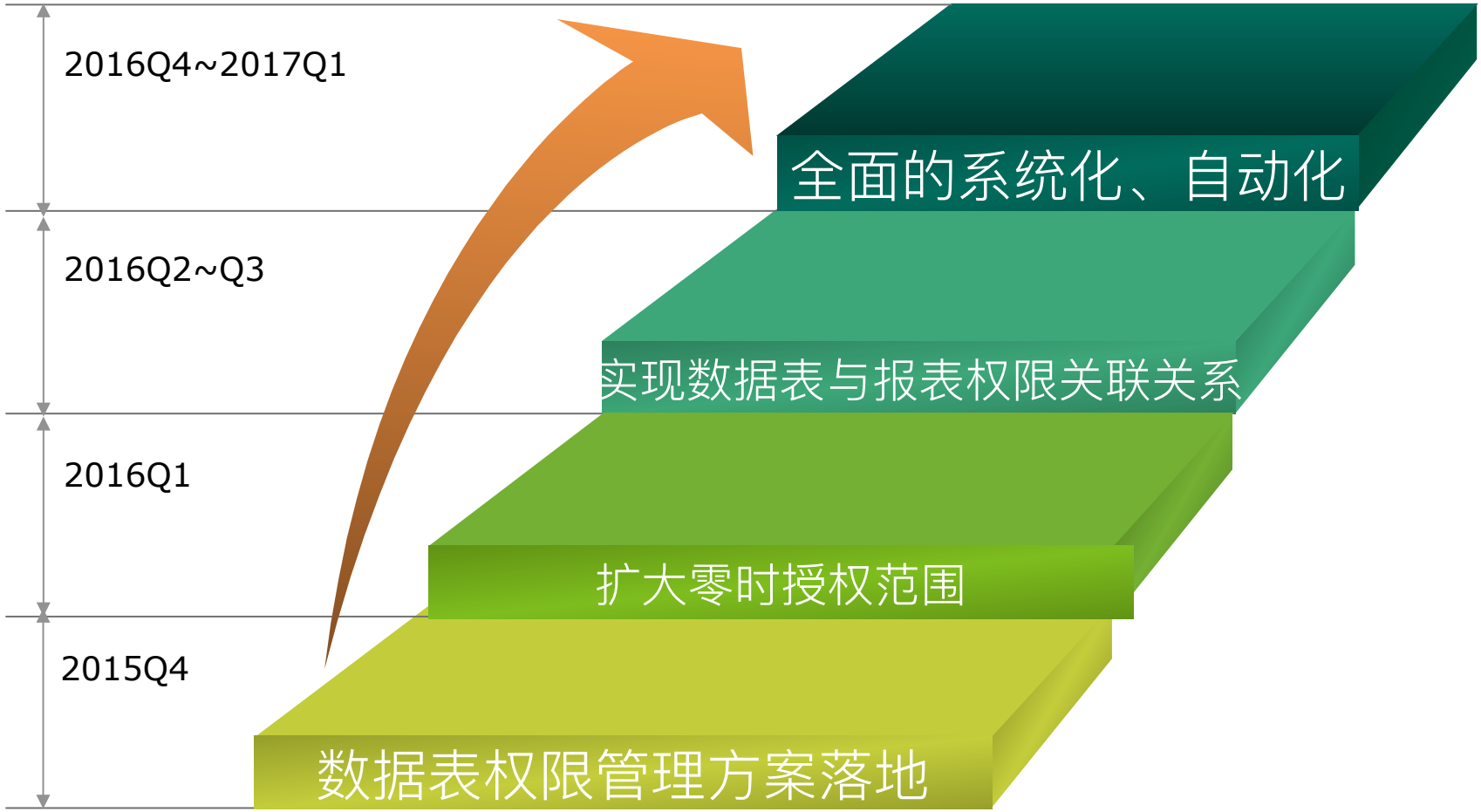


维度安全过滤器介绍

安全过滤器元素	功能	说明
filter: {id:$dim_id, in: $values}	设定控制的维度及维度值	id：表示维度元数据id in：表示控制维度值范围，为空则表示该维度没有查看的权限，不为空，即为查询阈值范围
highest_dim:{$h_id}	设置同维度层级上最高可以查看的维度	
lowest_dim:{$l_id}	设置同维度层级上最低可以查看的维度	默认为空
invalid_dims:{}	记录的是具有该权限所设置的限制条件	比如：BD经理可以查看同城市下其他的BD经理和BD的汇总数据，但是不能查看门店数据。即invalid_dims {$POI_id}

实现不可向上读

未来规划


2016Q4~2017Q1
2016Q2~Q3
2016Q1
2015Q4
全面的系统化、自动化
实现数据表与报表权限关联关系
扩大零时授权范围
数据表权限管理方案落地

QA